MISSISSIPPI ANALYSIS and INFORMATION CENTER (MSAIC)

PRIVACY POLICY

I. PURPOSE STATEMENT

The Mississippi Analysis and Information Center (MSAIC) was established to provide the information sharing and exchange of terrorism and crime-related information among members of the law enforcement community. The focus of the MSAIC is to combine the intelligence and information sharing efforts of all participating agencies to enhance the ability to predict, prevent, and respond to unlawful activity and threats to our nation. This is a process whereby information is collected, integrated, evaluated, analyzed and disseminated through established procedures for law enforcement purposes and in the interest of public safety. The intelligence products and services are made available to law enforcement agencies and other entities contributing to public safety throughout the state and country.

The MSAIC recognizes the importance of ensuring the protection of individual constitutional rights, civil liberties, civil rights, and privacy interests throughout the intelligence process.

II. DEFINITIONS

"Watch Center": the operations center consisting of analysts, watch officers, and other supervisors; synonymous with the MSAIC.

"Board of Directors": ***the group of individuals charged with providing guidance for the operations of the MSAIC to the Commissioner of Public Safety***

"Executive Director": manager appointed by the Commissioner of Public Safety/Director of Homeland Security to oversee the daily operations of the MSAIC.

"Stakeholder Agencies": those agencies that will participate in the operations of the MSAIC in addition to sharing and collecting information.

"Requestor": the individual law enforcement officer or agency making a request for information from, or reporting an incident to, the MSAIC; synonymous with "user."

"Reasonable Suspicion/Criminal Predicate" – when sufficient facts are established to give a trained law enforcement officer or employee a basis to believe there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise. (28CFR23)

"Personal Data" – any information relating to an identifiable individual.

III. INFORMATION COLLECTION

Personal data collected by the MSAIC will be retained in compliance with the Code of Federal Regulations (28 CFR 23), all pertinent Attorney General Guidelines, and any other applicable state, federal or local statutes governing the collection of intelligence information. Additionally, MSAIC will adhere to criminal intelligence collection guidelines established under the National Criminal Intelligence Sharing Plan (NCISP). Stakeholder agencies are responsible for ensuring the legal validity of gathered information to include the following minimal guidelines.

1. The source of the information is reliable and verifiable.

2. Information supports reasonable suspicion the individual or organization is involved in criminal conduct, and the information is relevant to that conduct.

3. Information was collected in a fair and lawful manner, with knowledge and consent of the individual, if appropriate.

4. Information may not be collected concerning political, religious or social views, associations, or activities of any individual, group, or organization unless the information directly relates to criminal conduct or activity, and there is reasonable suspicion the subject is involved in the illegal conduct.

5. Information is accurate and current per Code of Federal Regulations 28CFR23.

The MSAIC will abide by daily operating procedures for the initial collection and verification of intelligence, including the screening process by an analyst/call taker and the subsequent review by supervisory personnel.

The MSAIC is maintained for the purpose of developing information and intelligence for and by participating stakeholder agencies. The decision of the agencies to participate with the watch center and to decide which databases to provide for watch center access is voluntary and will be governed by the laws and rules governing those individual agencies, as well as by applicable federal laws.

IV. DATA QUALITY

The agencies participating in MSAIC remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the MSAIC. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. MSAIC personnel will endeavor

to ensure the accuracy of information received through database searches by cross-checks with other data systems and open source information. In order to maintain the integrity of the watch center, any information obtained through the watch center will be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data.

V. USE LIMITATION

Information obtained from or through the MSAIC can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation, or is a response to confirmed information that requires intervention to prevent a criminal act or threat to public safety.

The MSAIC will take necessary measures to ensure access to the watch center's information and intelligence resources is secure. Unauthorized access or use of the resources is forbidden. The Board reserves the right to restrict the qualifications and number of personnel having access to the watch center and to suspend or withhold service to any individual violating this *Privacy Policy*. The Board, or persons acting on its behalf, further reserves the right to conduct inspections concerning the proper use and security of the information received from the watch center.

Information disseminated by the MSAIC will be authorized on a "need to know" basis, and will be provided in accordance with applicable laws, rules, and regulations. Furthermore, all personnel who receive, handle, or have access to watch center data will be trained as to those regulations. All personnel having access to MSAIC data agree to abide by the following rules:

1. The watch center's data will be used only in support of official law enforcement activities.
2. Individual passwords will not be disclosed to any other person, except as authorized by MSAIC management.
3. Individual passwords of authorized personnel will be changed if the password is compromised or improperly disclosed.
4. Background checks will be completed on personnel who will have direct access to the watch center.
5. Use of the watch center's data in an unauthorized or illegal manner will subject the requestor to denial of further use of the watch center; discipline by the requestor's employing agency, and/or criminal prosecution.

The MSAIC Director reserves the right to deny access to any watch center user who fails to comply with the applicable restrictions and limitations of the watch center policy.

VI. SECURITY

Information obtained from or through MSAIC will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding signed with the participating agency. Information cannot be:

- sold, published, exchanged, or disclosed for commercial purposes;
- disclosed or published without prior approval of the contributing agency; or
- disseminated to unauthorized persons.

Research of MSAIC's data sources is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the watch center will be granted only to fully authorized personnel who have been screened with state and national fingerprint-based background checks, as well as any additional background standards established by the MSAIC Board with the approval of the Commissioner of Public Safety.

The MSAIC Director will identify technical resources to establish a secure facility for watch center operations with restricted electronic access, security cameras, and alarm systems to guard against external breach of the facility. In addition, the MSAIC Director will identify technological support to develop secure internal and external safeguards against network intrusion of watch center data systems. Access to the watch center's databases from outside of the facility will only be allowed over secure network lines.

VII. OPENNESS

It is the intent of the MSAIC and participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. Participating agencies will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation.

VIII. INDIVIDUAL PARTICIPATION

The data maintained by the MSAIC is obtained through participating stakeholder agencies, federal agencies, and open source resources. Individual users of watch center information are solely responsible for the interpretation, further dissemination, and use of information developed in the research process. Additionally, it is the responsibility of the user to ensure the accuracy, validity, and completeness of all intelligence information obtained prior to official action being taken in full or in part.

Members of the public cannot access personal information for themselves or others from the watch center applications. Persons wishing to access personal data pertaining to themselves should communicate directly with the agency or entity responsible for the data in question. Participating agencies agree that they will refer requests related to privacy back to the originator of the information.

IX. ACCOUNTABILITY

Queries made to the MSAIC data applications will be logged into the watch center's data system identifying the user initiating the query. When such information is disseminated outside of the originating agency, a secondary dissemination log will be created in order to capture updated information and provide an appropriate audit trail, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for investigative purposes or to other agencies as provided by law. The agency *from* which the information is requested will maintain a record of any secondary dissemination of information. This record should reflect at a minimum:

1. Date of release.
2. The subject of the information
3. To whom the information was released (including address and telephone number).
4. An identification number or other indicator that clearly identifies the data released.
5. The purpose for which the information was requested.

The MSAIC Governance Board with the concurrence of the Commissioner of Public Safety will be responsible for conducting or coordinating internal or special audits, and for investigating misuse of the watch center's information systems. All confirmed or suspected violations of MSAIC policies will be reported through the MSAIC Director to the Commissioner of Public Safety. Individual users of MSAIC information remain responsible for the appropriate use of watch center information. Each user of the watch center and each participating agency within the MSAIC are required to abide by this *Privacy Policy* in the use of information disseminated. Failure to abide by the restrictions for the use of the MSAIC data may result in the suspension or termination of user privileges; discipline imposed by the user's employing agency, or criminal prosecution.